一种能快速收敛的对等网络信任值计算算法

李治军[1], 廖明宏[1]

(1. 哈尔滨工业大学 计算机科学与技术学院, 哈尔滨 150001, E-mail: lizhijun_os@hit.edu.cn)

摘 要: 对目前对等网络中常用的信任值计算方法进行了形式化分析, 提出了一个分布式信任值迭代方法, 根据其特点命名为阻尼方法, 理论证明阻尼方法一定收敛. 在对阻尼方法收敛速度和安全性的分析基础上, 提出了一个结合了名誉管理、自适应调整的快速信任值计算算法(TVCA). 模拟实验表明TVCA算法在提高计算效率、抵抗恶意攻击等方面都能取得良好的效果.

关键词: 对等网络; 信任管理; 信任值计算

中图分类号: TP309 **文献标识码**: A **文章编号**: 0367-6234(2007)03-0457-05

A fast convergent algorithm for computing the trust value in peer-to-peer networks

LI Zhi-jun[1], LIAO Ming-hong[1]

(1. School of Computer Science and Technology, Harbin Institute of Technology, Harbin 150001, China, E-mail: lizhijun_os@hit.edu.cn)

Abstract: In the researches of the trust management of the peer-to-peer networks, the computing of trust value is most important. Typical algorithms nowadays for computing the trust value in peer-to-peer networks are formally analyzed. The results show that these algorithms can't produce the correct trust value. Therefore, a distributed iterative algorithm to compute the trust value called as damping method by its properties is provided. The formal analyses show that damping method must be convergent. Based on the analyses of the convergent speed and security of damping method, a fast convergent trust value computing algorithm or TVCA combining reputation management and self-adaptive adjustment is provided. The experimental results show that TVCA can achieve good effects in many aspects such as efficient computing and malicious attack resistance.

Key words: peer-to-peer network; trust management; trust value computing

P2P系统被广泛应用在诸如大规模信息共享, 分布式计算以及新型网络数据库等诸多领域上[1]. P2P信任管理[2-7]中的关键问题是结点可信度的计算, 计算该值的算法效果, 如准确程度, 计算效率等是决定系统上层安全性的关键因素. 如Aberer等人给出了通过对不成功应答信息的维护来检测恶意结点的方法[3]. NICE[4]给出了基于信任图来推导结点信任的方法; 文献[5]提出了基于商的信任值计算方法, 文献[6]提出了用贝叶斯网来构建信任管理模型; EigenTrust[7]是基于成功应答和不成功应答的差值来计算信任值的. 上述研究均存在不能获得信任度准确值及未对其正确性和效率因素进行分析的缺点. 对于P2P信任值的计算, 需满足如下3个基本要求: 准确、高效、安全性高[3-7]. 由于P2P系统的自治性, 所以, 对结点的可信程度的认识是一个不断深入的过程, 一般都是通过迭代调整来接近准确值. 准确是指最终可以收敛到结点可信程度的真实值, 效率是指收敛速度. 除了上述两个基本特性以外, 由于信任值的计算常常是作为上层安全系统构建的基础, 所以, 就可能存在对信任值计算的攻击, 如何保证信任值计算本身的安全性也是一个重要的指标.

本文在对目前的典型信任值计算方法进行了形式化分析的基础上, 提出了一种可收敛的信任

收稿日期: 2005-11-14.
基金项目: 哈尔滨工业大学校基金(HIT2002.74).
作者简介: 李治军(1977—), 男, 讲师, 博士;
廖明宏(1966—), 男, 教授, 博士生导师.

值计算方法,并对这一方法的效率进行了分析,另外,也考虑它的安全性,给出了一个可以快速收敛的信任值计算算法,实验证明这一算法具有良好的效果.

1 现有典型信任值计算方法的分析

1.1 线性的信任值计算方法(LT)

线性信任(LT)基本计算形式为

$$Tr_{AB}^{n} = Tr_{AB}^{o} + e\Delta T. \tag{1}$$

其中: e用来反映信息交互结果,成功时为 1,失败为 -1;而 ΔT为信任值调整量,且 $\Delta T > 0$ 也有一些模型,如 NICE模型[4]采用这种方法.

最终收敛到的信任值表现为当交互次数达到无穷大时,由式(1)迭代得出的结果.显然对于式(1),当交互次数无穷大时有

$$Tr_B = Tr_{AB}^{o} + \Delta T \cdot \lim\left(\sum e\right) = \pm\infty.$$

可以看出式(1)最终不收敛.

1.2 基于商的信任值计算方法

采用除法是信任值计算的另一种常见的方法,如文献[5],其基本计算形式为

$$Tr = GA/TA.$$

其中: GA 是成功行为的计数值, TA 为所有行为的计数值,由于这种形式给出的结果不易分析,可将其转化为如下迭代形式:

$$Tr_{AB}^{n} \approx Tr_{AB}^{o} + e/TA. \tag{2}$$

TA越大时,式(2)的左边和右边越接近.显然式(2)和式(1)是完全一样的,也不能收敛到真实的信任值.

1.3 基于幂的信任计算方法(ET)

文献[6]提出了如下的信任值计算方式:

$$Tr_{AB}^{n} = \alpha \cdot Tr_{AB}^{o} + e \cdot \beta$$

其中: α, β满足 $(0 \leqslant \alpha, \beta \leqslant 1)$,且通常有 $\beta = 1 - \alpha$ 对此式分析可得

$$Tr_B = (1-\alpha) \cdot \lim\left(\sum e_i \cdot \alpha^{n-i}\right). \tag{3}$$

显然信任值的计算最终转化为幂的形式,所以根据其特点,可将其称为幂信任(ET).由于式(3)不直观,所以图1给出了当 $s = 0.6$, $\alpha = 0.9$ 时对此种信任值计算方式迭代情形的图示,其总的修正次数分别为 10, 10^2, 10^3, 10^4. 从图1可以看出,该修正方法最终不能收敛于 0.6,而是在近似于 $[-0.6, 0.6]$ 的区间上振荡.对于其他的 (s, α) 组合,结果相同.

2 阻尼信任值计算方法

从以上分析结果可以看出,常见的许多信任值计算方法都不能收敛到目标结点可信程度的真实值.为此本文提出一个可证明其收敛性的信任值计算方法

$$Tr_{AB}^{n} = Tr_{AB}^{o} + e \cdot \Delta T \cdot \left(\frac{1}{i-1} - \frac{K(i) - L(i)}{i(i-1) \cdot e}\right). \tag{4}$$

其中: K 和 L 是两个计数函数,其自变量为信息交互次数 i, K 和 L 分别定义为:若 $e = 1$ 则 $K(i+1) = K(i) + 1$, $L(i+1) = L(i)$;若 $e = -1$ 则 $K(i+1) = K(i)$, $L(i+1) = L(i) + 1$;其初值为 $K(0) = L(0) = 0$

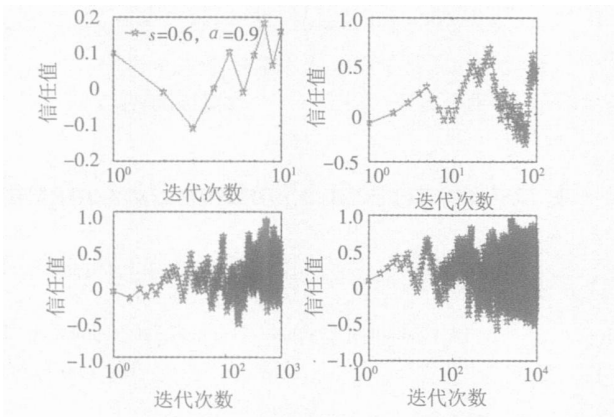


图1 ET的结果图示 ($s = 0.6$)

式(4)的迭代结果如图2所示,可以看出,该计算方法最终能够收敛到可信度的真实值,且收敛过程与阻尼振荡过程十分类似,故将其称为阻尼信任(DT).

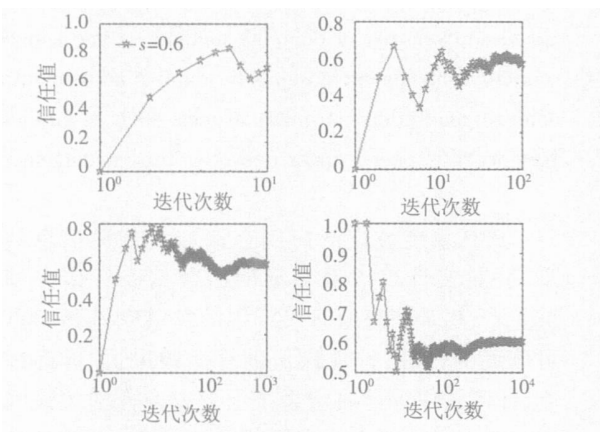


图2 DT的结果图示 ($s = 0.6$)

定理 1 DT算法可收敛到真实的可信度.

证明 定义两个数列: $a_1(n) = -1/(n(n-1))$, $a_2(n) = e$,显然有: $S_1(n) = 1/n$, $S_2(n) = (2s-1)n$.

定理的证明相当于构造一个数列,使 $S(n) = S_1(n) \cdot S_2(n)$. 此时,可求得结果数列的通项为 $a(n) = e/(n-1) - n(2s-1)/(n(n-1))$,由于该式中的 $n(2s-1)$ 是不能直接得到的,但可表示

为 n次交互中成功次数与失败次数的差, 在第 i次交互时此值为 $K(i) - L(i)$.

由以上分析可知, 对于式 (4) 有

$$Tr_{AB} = Tr_{AB}^{0} + \Delta T \cdot \lim S(n) = 1/2 + \Delta T \cdot (2s - 1).$$

取 $\Delta T = 1/2$, $Tr_{AB} \to s$, 从而式 (4) 收敛于 s.

3　阻尼信任值计算方法的分析

3.1　收敛速度分析

定理 **2**　DT的收敛速度是所有可收敛信任值计算算法收敛速度的上界.

证明　由阻尼信任计算的迭代公式可以看出, 该公式反映的是交互成功与否的和式. 其收敛速度取决于该和式反映 s的速度. 由于 s只能通过这样的和式才能反映出来, 所以显然 DT方法的收敛速度是所有可收敛信任值计算算法收敛速度的上界, 且其收敛速度与值 s无关.

定理 2决定了不可能通过构造其他修正公式来提高收敛速度, 所以收敛速度的提高只能在式 (6)的基础上进行, 若要加速收敛, 只能提高交互数量. 而在任何一段时间内, 针对结点 B 的交互数量是一定的, 且该数量只和系统中的结点有关, 本文是一个不变量. 但是, 和 B 的交互是系统中多个结点共同完成的, 而系统中结点对 B 的可信度的刻画时间取决于相应的分摊数量, 所以, 加速这一收敛速度的一个直观想法就是系统的结点能共享和 B 的交互经验, 这就是名誉机制要解决的问题.

3.2　安全性分析

由于 P2P系统的开放性, 所以在系统中必定会存在大量的恶意结点. 对于信任管理机制而言, 恶意结点并不是指安全性低的结点, 而是指那些以较高的可信度工作了一段时间后突然降低其可信度的结点, 由定理 1可以看出, 虽然此时 DT也能收敛到变化后的信任值, 但此时的收敛速度将会下降到

$$n_2 \geqslant \frac{n_1 \cdot (|s_1 - s_2| - \delta)}{\delta}. \qquad (5)$$

其含义为若结点以信任值 s_1 进行了 n_1 次交互后变为 s_2, 此时最少需进行 n_2次交互后刻画得到的安全势将和 s_2 的差值不超过 δ从式 (5) 可以看出 n_2受 δ的影响最大, 即使 δ取一个较大数 (如 0.1), n_2也远大于 n_1 ($n_2 = 10n_1$). 这说明 DT方法对可信度的变化不敏感. 从式 (5) 可以看出, 变化敏感性的提高关键在于 n_1 的处理, 若能够保证在刻画 s_2 时, $n_1 = 0$, 那么 n_2就能达到最小. 相应的方法就是在适当时刻对结点可信度进行重新刻画, 这一时刻可以是周期性的, 也可以是事件驱动的.

4　快速的信任值计算算法 (TVCA)

提出一个能快速收敛的信任值计算算法: TVCA (Trust Value Computing Algorithm). TVCA的结构如图 3所示, 主要包含 3个模块: 信任计算、名誉机制、自适应重调整. 其中名誉及信任的表示可直接采用已有的方法[3~7], 但信任值的计算采用的是 DT方法. 图 4和 5分别给出了 TVCA中的名誉算法和自适应重调整算法.

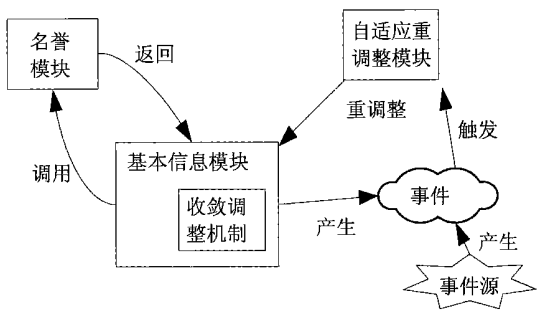


图 3　TVCA算法的结构

```
算法:TVCA_ReputaionAlgorithm
输入:(A,B,W(B))
/*A:发起者;B:被考察者;W(B):B行为的目击者*/
输出:R(B)/*R(B)为B的名誉*/
Peer A:
for p∈W(B)
    A. Send(p,Request(Reputation,B));
wait;
Peers W(B):
    p. Send(A,Response(TSpB,TrpB,ipB))
/*TSpB为B的调整时间戳,ipB为p与B的交互次数*/
Peer A:
P = A. Select(TrpB * ipB > trBound) ∩
    A. Select(TSpB > TSAB || (TSAB - TSpB) < tBound)
R(B) = (∑_{p∈P} TrAp × TrpB × ipB) / (∑_{p∈P} TrAp × ipB).
```

图 4　TVCA中的名誉考虑 法 (TVCA_RA)

算法 TVCA_RA 中 $W(B)$ 的选取可以有多种方法, 可以是和 B 相似的结点集, 也可是 A 的邻居结点集, 当然也可是 A 最信任的结点集, 等等. 此处选取 $W(B)$ 为 A 的邻居结点集. 在算法 TVCA_RA 中, 为克服未调整结点对新调整结点的影响, 特引入时间戳, 只考虑在一定时间范围内的信息. 同样的, TVCA_RAA 算法中的触发事件也可以有多种, 此处主要讨论周期事件 (Period) 和信任值跳跃检测事件 (TrustJump). 周期事件中的周期选

取将通过实验确定;信任值跳跃检测事件可通过结点对信任值的变化幅度来触发.

```
算法:TVCA _ ReAdjustAlgorithm
输入:Event/ * 触发重调整过程的事件 * /
输出:无
Peer A;
if Event. IsTypeOf( Period) / * 周期事件 * /
    for p ∈ I( A) / * I( A) 表示和 A 有交互的结点集 * /
    if( p. i > iBound)
      A. ReSet( p. i, p. K( i) , p. L( i) ) ;
      A. Tag( p, TimeStamp( ReAdjust) ) ;
      / * 打上重调整时间戳 * /
if Event. IsTypeOf( SecurityJump( B) )
      / * B 安全势的跳跃检测事件 * /
    A. ReSet( B. i, B. K( i) , B. L( i) ) ;
    A. Tag( B, TimeStamp( ReAdjust) ) ;
```

图 5 TVCA 中的重调整算法(TVCA_RAA)

5 实验结果及分析

TVCA 算法的实验是在一 P2P文件共享模拟平台上进行的. 模拟时假定系统中有 N 个 Peer, 每个 Peer都能发起查询和应答查询. 假定系统中的文档近似均匀地随机分布在 N 个结点上. 实验中采用的是基于信任的查询算法, 并由查询发起者决定该向哪些结点发出查询, 其他结点只完成路由. 假设系统中任何时刻都有% η的结点发起查询.

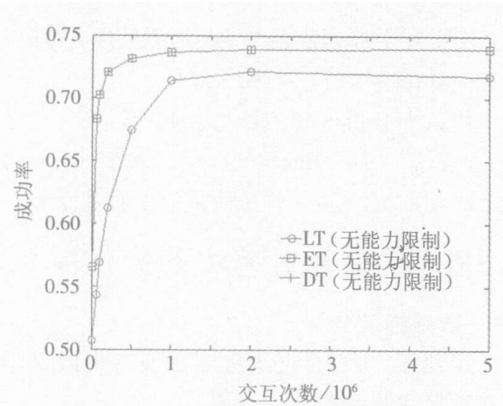
5.1 DT算法对安全性的提高

将系统的安全性定义为交互的成功率. 在模拟实验中考虑结点的处理能力为 C.

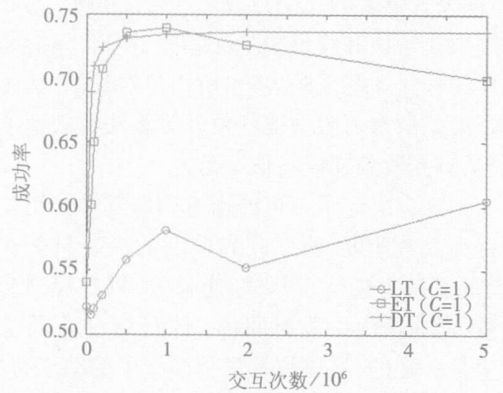
图 6对 LT, ET, DT3种信任值计算方法进行了安全性比较, 可以看出, DT的收敛速度明显要快得多; 在不考虑结点能力限制时, DT 的安全性和 ET一样, 而比 LT高. 当限制了结点的能力时, ET安全性很快下降, 而 DT 安全性几乎不变. 当能力限制变强 (C = 1)时, LT 和 ET的安全性在达到某极大点后都明显下降, 该点为近似可信度, 过了该点后对可信度的刻画将背离真实情况, 而对 DT 则会收敛在此真实值上. 当能力限制很强时 (C = 0.5), ET、LT的安全性不断下降, 直至很小, 而 DT最终仍能收敛到一个较为安全的情况.

5.2 TVCA_RA对信任值计算的影响

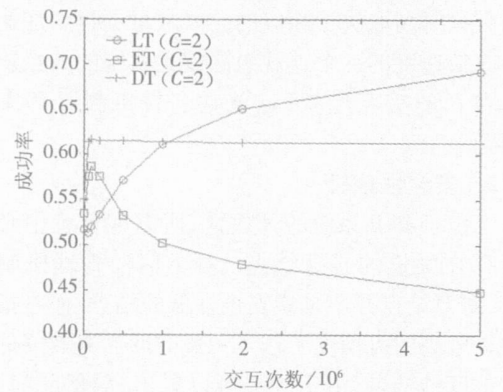
图 7显示了 TVCA_RA 对信任值计算的影响, 给出了计算值和真实值之间的差别 (用二者的距离 D 表示). 由图 7可知名誉机制可以使信任值很快收敛, 同时, 由于名誉机制的影响, 信任值不能无限制收敛, 这是由于其他结点的不正确判断所产生的负面影响.



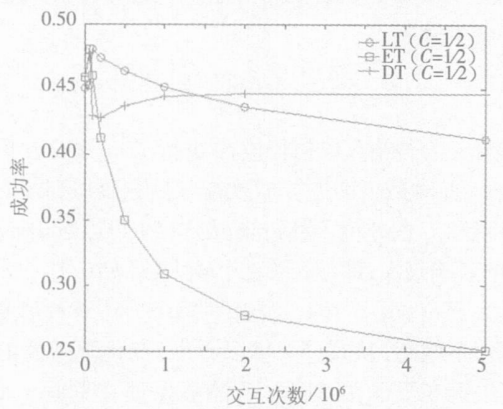
(a) 三种算法在无能力限制时的安全性比较



(b) 三种算法 C = 1 时的安全性比较



(c) 三种算法在 C = 2 时的安全性比较



(d) 三种算法在 C = 1/2 时的安全性比较

图 6 三种算在各种 C 下的安全性比较

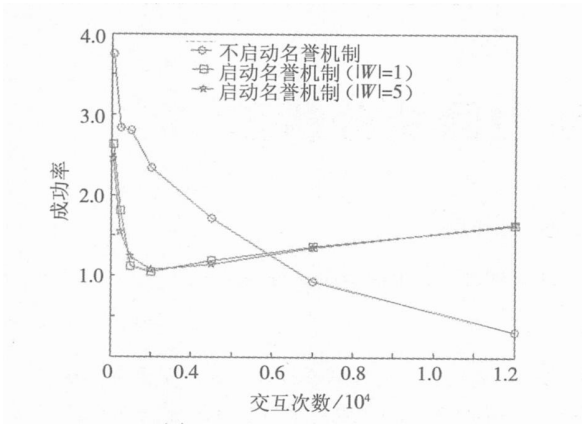


图 7　*TVCA_RA* 的影响

6　结　语

对典型的信任值计算方法进行了形式化分析，提出了一个分布式信任值计算算法，并证明了该算法一定能够收敛到可信度的真实值上．同时对该算法的收敛速度和安全性都进行了深入的分析．大量的模拟试验证明，该算法可以取得良好的效果．

参考文献：

[1] ANDY O. Peer-to-Peer: Harnessing the Power of Disruptive Technologies[M]. [s.l.]: O'Reilly & Associates, Inc., 2001: 3－159.

[2] WALLACH D S. A Survey of Peer-to-Peer Security Issues[C]. In International Symposium on Software Security. Tokyo: Springers, Inc, 2002: 42－57.

[3] ABERER K, DESPOTOVIC Z. Managing trust in a peer-2-peer information system[C]//Ninth international conference on information and knowledge Management. Georgia: ACM Press, 2001: 310－317.

[4] SHERWOOD R, LEE S. Cooperative peer groups in NICE[J]. The International Journal of Computer and Telecommunications Networking, 2006, 50(4): 523－544.

[5] STAKHANOYA N, FERRERO S. A Reputation-based Trust Management in Peer-to-Peer Network Systems[C]//Security Workshop of International Conference on Parallel and Distributed Computing Systems. San Francisco: IEEE Computer Society, 2004: 510－515.

[6] YAO W, JULITA V. Trust and reputation model in peer-to-peer networks[C]//Proc. of the 3rd IEEE Int'l Conf. on Peer-to-Peer Computing. Linköping: IEEE Computer Society, 2003: 150－158.

[7] KAMVAR S, SCHLOSSER M. The EigenTrust Algorithm for Reputation Management in P2P Networks[C]//Proc. of Int'l Conf. on World Wide Web. Budapest: ACM Press, 2003: 640－651.

(编辑　杨　波)

(上接第 456页)

[23] BRYANT S, WANG Feiyi. Aspects of adaptive reconfiguration in a scalable intrusion tolerant system[J]. Complexity, 2004, 9(2): 74－83.

[24] LIU P, JAJODIA S, MCCOLLUM C D. Intrusion confinement by isolation in information systems[J]. Journal of Computer Security, 2000, 8(4): 243－279.

[25] LIU P, AMMANN P, JAJODIA S S. Rewriting Histories: Recovering From Malicious Transactions[J]. Distributed and Parallel Databases, 2000, 8(1): 7－40.

[26] YU M, LIU P, ZANG Wanyu. Multi-Version Attack Recovery for Workflow Systems[C]//19th Annual Computer Security Applications Conference. Las Vegas, Nevada: [s.n.], 2003.

[27] 闵应骅，网络容错与安全研究述评[J]．计算机学报，2003, 26(9): 1035－1041.

[28] REITER M K, BIRMAN K P. How to securely replicate services[J]. ACM Transactions on Programming Languages and Systems, 1994, 16(3): 986－1009.

[29] CASTRO M, LISKOV B. Practical Byzantine Fault Tolerance[C]// In 3rd Symp. on Operating System Design and Impl. New Orleans, USA: [s.n.], 1999: 173－186.

[30] REITER M K. Distributing trust with the Rampart toolkit[J]. Communications of the ACM, 1996, 39(4): 71－74.

[31] KIHLSTROM K P, MOSER L E, MELLIAR-SMITH P M. The SecureRing protocols for securing group communication[C]//In Proc 31st Hawaii International Conference on System Sciences, Kona, Hawaii [s.n.], 1998: 317－326.

[32] MOSER L E, MELLIAR-SMITH P M. Byzantine－resistant total ordering algorithms[J]. Information and Computation, 1999, 150(1): 75－111.

[33] DOUDOU A, GARBINATO B, GUERRAOUI R. Abstractions for devising Byzantine－resilient state machine replication[C]//In Proc 19th Symposium on Reliable Distributed Systems (SRDS 2000). Nuremberg, Germany: [sn.], 2000: 144－152.

[34] MALKHI D, MERRITT M, RODEH O. Secure reliable multicast protocols in a WAN[J]. Distributed Computing, 2000, 13(1): 19－28.

[35] GANGER G R, KHOSLA P K, BAKKALOGLU M. Survivable Storage Systems[C]//DARPA Information Survivability Conference and Exposition. Anaheim, USA: [s.n.], 2001: 184－195.

(编辑　王小唯)